
دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

التفتيش في الجرائم المعلوماتية [1]

DOI:10.12816/0000352

الدكتور. عادل عبدالله خميس المعمري [2]

أستاذ القانون الجنائي المشارك – جامعة عجمان للعلوم والتكنولوجيا - الإمارات

مستخلص

يعتبر التفتيش من الإجراءات الهامة في الدعوى الجزائية باعتباره إجراء من إجراءات التحقيق الابتدائي ، الذي يساعد كدليل مادي مهم في الكشف عن الحقائق في هذا الموضوع. ولذلك نظر الباحث لهذا الموضوع وتناوله من الجانب الإلكتروني لأنه موضوع الساعة ، حيث أن معظم الجرائم في الوقت الحالي تستعمل فيها الأجهزة الإلكترونية التي يصعب ضبط الدليل فيها ؛ لسهولة وسرعة إخفاء المعلومات. وتبدو إشكالية هذه الدراسة في عدم وجود تشريع إجرائي في الإمارات ينظم الإجراءات الجنائية الخاصة بجمع الاستدلالات وضبط الجرائم المعلوماتية كما تكمن الصعوبة الأخرى في وجود نقص في خبرة رجال الضبط في مجال الكشف عن هذه الجرائم ، ولقد تم اعتماد المنهج الاستقرائي التحليلي بحيث قام الباحث بعرض نماذج من القوانين العربية مقارنة ببعض التشريعات الأجنبية والقانون الإماراتي. وقد تناول هذا البحث في فصلين ، حيث تناول في الفصل الأول موضوع التفتيش ، وتعريفه ، وخصائصه ، وكيف يتم ، ثم ماهيته وتعريف التفتيش الإلكتروني وشروطه سواء الشكلية أو الموضوعية. أما في الفصل الثاني فقد تم التركيز على آثار التفتيش والأدلة الإلكترونية ، وكيفية تفتيش هذه الأدلة ومن هي الجهة المسؤولة عن هذا التفتيش. وقد أظهرت الدراسة شروطاً موضوعية لتفتيش النظام المعلوماتي أهمها وجود سبب لإجراء التفتيش وتحديد محل التفتيش وأن يكون الأمر الصادر بالتفتيش كتابياً وموقعاً ومؤرخاً ومحدد المدة والنطاق وأن يتم علم محضر بإجراءات ونتائج التفتيش وخلص البحث في النهاية إلى عدة نتائج: 1. النظر في إصدار قانون اتحادي إجرائي في مجال الإجراءات مثل التفتيش والقبض وبالذات المجال الإلكتروني لوجود صعوبة في بعض الأحوال في تطبيق قانون الإجراءات في موضوع الأدلة الإلكترونية مثل خصوصية التفتيش في مجال الأجهزة الإلكترونية. 2. تدريب أفراد الشرطة على عمليات ضبط وتحريز الأجهزة الإلكترونية وعمل دورات تخصصية لهذا الموضوع. 3. مما لا شك فيه أن للإعلام دوراً مهماً في هذا الموضوع ، وهو توعيـــة الجمهور بأهمية هذا الموضوع من ناحية خطورة هذه الأجهزة وأهميتها ، وكيف تنقل المعلومات وكيف تتم سرقتها.

مفردات البحث :

التفتيش — الجرائم المعلوماتية — الدليل الإلكتروني — الحاسوب الآلي — أجهزة الاتصال — التحقيق الابتدائي — ضبط الأدلة — ضبط المراسلات البريد الإلكتروني — المراقبة الإلكترونية — مراقبة المحادثات الهاتفية.

1- ورد هذا البحث للدورية في يناير 2013م وقيد تحت رقم 2013/36 وأحيل للتحكيم في فبراير 2013م وأجيز للنشر في مارس 2013م.

2- حصل الدكتور عادل عبدالله خميس جمعة المعمري على درجة الدكتوراه في القانون الجنائي من جامعة المنصورة عام 2001م ، كما عمل 31 عاماً في دوائر شرطة الشارقة ، وحالياً أستاذ القانون الجنائي المشارك في شبكة جامعة عجمان للعلوم والتكنولوجيا ، كما يعمل محامياً ومستشاراً قانونياً بمكتبه الخاص بإمارة الشارقة ، وشارك في عدة دورات متخصصة ، وعمل على إعداد بحوث وكتب في مواضيع مختلفة.

Search in Information Crimes [1]

DOI:10.12816/0000352

Dr. Adil Abdullah Khamis Al Muamari [2]

Associate Professor of Criminal Law

Ajman University of Science and Technology- UAE.

Abstract:

Being one of the procedures followed in initial investigation, search is considered to be a general procedure in criminal lawsuits. It is a crucial physical evidence in the detection of crimes. The study deals with electronic search owing to the fact that most criminals nowadays employ electronic devices in their crimes making it harder to collect evidence; as information can be easily concealed. There are no any procedural legislation in UAE regulating criminal procedures of evidence collection and detection of crimes; which is one of the questions raised by study. Another question is the inexperience of police personnel in the detection of such crimes. Inductive analytical approach is used by the study by which some Arabic laws, including UAE's ones were compared with foreign ones. Study consists of two sections; the first one sets forth the definition of search along with its characteristics and the way of conducting it. It also sets forth definition of electronic search and its conditions. The second section deals with the collection of electronic evidences and the body authorized to carry out this job. Study enumerates a number of conditions for the search of information system; the most salient are that there should be a reason behind the inspection or search; inspection place should be located; obtaining a written and dated search warrant and finally preparation of a report on the search's findings. Study sums up with the following recommendations: 1. Enacting a federal procedural law in the field of search and seizure in cybercrimes. 2. Providing police personnel with training on seizure and confiscation of electronic devices by means of organizing specialized training courses. 3. Activating the role of media in raising peoples' awareness to risks of cybercrimes.

Keywords:

Search – Information crimes – Electronic Evidence – Computer – Communication Devices – Initial Investigation – Evidence Collection Email Correspondence Control- Electronic Surveillance - Telephone Calls' Monitoring.

1-**Manuscript:** was submitted in January 2013 (under No (36), refereed in February 2013 and approved for publication in March 2013.

2-**Biography:** Dr. Adil attained his PhD from Mansoura University in 2001. He has been working for Sharjah Police for 31 years. Presently he is an associate professor of Criminal Law at Ajman University of Sciences and Technology. He is also an advocate and legal consultant running his private office in Sharjah. He has taken part in a host of specialized training courses, and authored a number of researches and books in miscellaneous legal topics.

مقدمة :

يعتبر التفتيش من الإجراءات الهامة في الدعوى الجزائية باعتباره إجراء من إجراءات التحقيق الابتدائي الذي يساعد كدليل مادي مهم في الكشف عن الحقائق في هذه الدعوى. ولهذا السبب تنص عليه معظم التشريعات على اعتبار أنه ماس بحرية الإنسان سواءً البدنية أو السكنية أو المعلومات الخاصة بالجرائم المعلوماتية في الانترنت والحاسب الآلي. ولقد اهتمت معظم دول العالم بالقوانين والتشريعات الإجرائية التي ينبع منها التفتيش وقواعده ، وعلى ذلك فإن السبب الرئيسي من النص على قواعد التفتيش هو اعتباره ضمانة مهمة للمتهم من جهة ولتحقيق العدالة من جهة أخرى ولهذا وضعت له التشريعات جزاء وضمانة مهمة وهي بطلان إجراءاته إذ يعتبر الإجراء باطلاً بطلاناً مطلقاً وذلك لاعتباره من قواعد النظام العام وفي إجراءات أخرى يعتبر بطلانه بطلاناً نسبياً.

وتعد الجرائم المعلوماتية عن طريق الانترنت من أخطر الجرائم في الوقت الحالي مثل جرائم الحاسب الآلي الخاصة بحرية الإنسان الشخصية كبطاقات الائتمان التي تحتوي على معظم المعلومات الخاصة بالعميل في البنوك وحساباته ، وكذلك جرائم سرقة المعلومات وبالذات الاستخباراتية على مستوى دول العالم ، والتي تحاول وضع حماية خاصة وتعاقب عليها بأشد العقوبة ومما لا شك فيه أن العالم أصبح قرية صغيرة وأن المعلومات تتوفر بأسرع ما يمكن وبالتأكيد فإن هذه الجرائم تختلف عن الجرائم العادية شكلاً وموضوعاً حيث من الممكن إتلاف الدليل الجنائي في أي لحظة.

ومن هذا المنطلق فإني اخترت هذا الموضوع المهم لأنه كما ذكرنا سابقاً يعتبر من الجرائم الهامة التي تحتاج الى دقة وخبراء مختصين لإخراج هذه الأدلة الهامة أثناء التفتيش عن المعلومات الجنائية الإلكترونية.

إشكالية الدراسة:

تكمن إشكالية هذه الدراسة في النقاط الآتية :

1. لا وجود لتشريع إجرائي إماراتي ينظم الجوانب الإجرائية عند ارتكاب جريمة معلوماتية.
2. اختلاف التفتيش في الجرائم التقليدية عن الجرائم المعلوماتية اختلافاً كاملاً ومؤثر وجذرياً.
3. صعوبة تفتيش أجهزة الحاسب الآلي المرتبطة بجهاز المتهم الذي يحتوي على المعلومات والأدلة الخاصة بالتفتيش.
4. نقص الخبرة لدى المحققين ورجال الضبط القضائي في مجال الكشف عن هذه المعلومات.
5. إحجام أكثر الضحايا في هذه الجرائم عن الإبلاغ عن هذه الجرائم كما يحدث في حالة القرصنة التي تتعرض لها المؤسسات المالية الكبيرة.

أهمية الدراسة:

مما لا شك فيه أن الجرائم المعلوماتية تعتبر من أحدث وأهم الجرائم في هذا الوقت ، فهي تحتاج إلى قانون إجرائي وعقوبات معينة أي قانون موضوعي وتكمن أهمية الدراسة في بذل الجهد لوضع حلول للمشكلات القانونية والفني التي تقف في طريق إجراء التفتيش في الجرائم المعلوماتية. وإغلاق أي ثغرة موجودة في هذا المجال ووضع الحلول الملائمة لسد هذه الثغرات وكل ذلك يتطلب بعض الاتفاقات العالمية وبعض القوانين العربية التي تحت منحى في هذا الموضوع والمطالبة بقانون وتشريعات إماراتية إجرائية في جرائم المعلومات الإلكترونية.

منهجية الدراسة:

سوف اعتمد في دراستي هذه على المنهج الاستقرائي التحليلي بحيث أنني سوف أعرض نماذج من القوانين العربية وبعض القوانين الأجنبية والقانون الإماراتي بالذات.

محتوى الدراسة:

سوف نقسم الدراسة إلى فصلين ، في الفصل الأول سوف نتناول التعريف بالجرائم المعلوماتية وسوف نتحدث في ثلاثة مباحث ، المبحث الأول مفهوم المعلوماتية ثم نتحدث في ثلاثة مطالب الأول : تعريف المعلوماتية والمطلب الثاني : خصائص الجرائم ، والمطلب الثالث : محل الجرائم المعلوماتية ، ثم نتناول في المبحث الثاني ماهية التفتيش في الجرائم المعلوماتية وسوف نقسمه إلى مطلبين الأول يتناول معنى التفتيش القضائي وخصائصه وفي المطلب الثاني سوف أتطرق إلى صور التفتيش غير القضائي وذاتيته. أما في المبحث الثالث فسوف نتناول شروط التفتيش في الجرائم المعلوماتية وسوف نتناوله في مطلبين المطلب الأول سوف ندرس الشروط الموضوعية للتفتيش في المطلب الثاني الشروط الشكلية للتفتيش أما في الفصل الثاني فسوف نتناول آثار التفتيش في الجرائم المعلوماتية. ففي المبحث الأول سوف نتطرق إلى ضبط الأدلة في مطلبين الأول يتعلق بقواعد ضبط الأدلة ، أما المطلب الثاني فسيكون المراقبة الالكترونية ثم الخاتمة والنتائج والتوصيات.

الفصل الأول
التعريف بالجرائم المعلوماتية

مع منتصف القرن العشرين حدثت قفزة نوعية في مجال العلوم قاطبة ، وكان على رأسها ثورة المعلومات التكنولوجية وكان اختراع الحاسب الآلي الذي كان له تأثير مباشر على حياة الإنسان اليومية ، بحيث لا يخلو مكان دون وجوده فأصبح موجوداً في كل المجالات لتبادل المعلومات الهامة ، والارتباط بين شبكات المعلومات كان له تأثير مهم في تبادل المعلومات ، فأصبح الكبير والصغير يستطيع أن يقرأ ما يدون في العالم صباحاً ومساءً وكنا نقول أن العالم أمسى قرية صغيرة واقتربت المسافات بين الدول بفضل وسائل المواصلات ، ولكن الآن نستطيع أن نقول أن العالم يكون دولة واحدة بسبب الأنظمة المعلوماتية الحديثة من وسائل المعلومات المتطورة في جميع المجالات من انترنت وشبكات المعلومات الدولية ، من هذا المنطلق برز أشخاص استعملوا هذه الشبكة المعلوماتية من

الجانب الآخر ألا وهو الجانب السلبي الذي ينتهك الحياة الخاصة للأفراد والناس أي يدخل في خصوصياتهم ، وقد ارتكبت جرائم كثيرة بسبب الاستعمال السلبي لهذه الشبكة المعلوماتية كجرائم سرقة المعلومات الهامة من الدوائر الحكومية والشركات الخاصة ، وكذلك أخذ صور بعض الفتيات ونشرها عبر الشبكة وكذلك الاعتداء بألفاظ نابية على شخصٍ معين. وحتى استعمال بطاقات الائتمان الالكترونية وسرقتها وتزويرها.

ولهذا كان لا بد من تضافر الجهود سواء المحلية أو الدولية لحل هذه المشكلة عن طريق تشريع إماراتي قوي يواجه هذه الجرائم الخطيرة ، ولهذا كله وتمهيداً للوصول الى موضوعنا الرئيسي وهو التعريف بالتفتيش المعلوماتي سوف نتناول في هذا الفصل في المبحث الأول مفهوم الجرائم المعلوماتية ومحلها ثم نتناول في المبحث الثاني ماهية التفتيش في الجرائم المعلوماتية وسوف أقسم هذا المبحث إلى مطلبين أتحدث في المطلب الأول عن معنى التفتيش القضائي وخصائصه وفي المطلب الثاني سوف نتطرق إلى صور التفتيش غير القضائي وذاتيته.

المبحث الأول - مفهوم الجرائم المعلوماتية:

سوف نقسم هذا المبحث إلى مطلبين الأول يتناول التعريف بالجرائم المعلوماتية ونذكر في المبحث الثاني خصائص هذه الجرائم.

المطلب الأول – تعريف الجرائم المعلوماتية:

لقد اختلف الفقهاء الجنائيين في تعريف المقصود بالجرائم المعلوماتية ، لذلك اتجه البعض في تعريف هذه الجرائم عن طريق الاستناد إلى وسيلة ارتكاب الجريمة ، أما البعض الآخر فقد استند إلى موضوع هذه الجرائم ، وهنالك اتجاه آخر عرفها على أساس المعرفة الفنية باستخدام الحاسوب ، ويوجد اتجاه آخر استند إلى أكثر من معيار واحد للتعريف وقد أخذ بالاتجاهات الأخرى المذكورة.

الرأي الأول: يرى هذا الرأي أن الجرائم المعلوماتية تعرف بالرجوع إلى وسيلة ارتكاب هذه الجريمة : ويأخذ هذا الاتجاه في تعريفه للجريمة المعلوماتية وسيلة ارتكاب الجريمة فهو عرفها بأنها " كل اشكال السلوك غير المشروع أو الضار بالمجتمع ، والذي يرتكب باستخدام الحاسب الآلي والإنترنت " (1). وكذلك عرفت بأنها " الفعل الإجرامي الذي يستخدم في اختراقه الحاسب الآلي كأداة رئيسة " (2). ويوجد تعريف آخر على أساس " الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي الإلكتروني". إن الذين اعتمدوا على أن وسيلة ارتكاب الجريمة هي التعريف للجرائم المعلوماتية انتقدوا لأن الجرائم المعلوماتية تقوم في الأساس على العمل الرئيسي المكون لها وليس فقط على الأداة التي استخدمت ، لذلك فإنه لا يمكن تعريف الجريمة على أنها جريمة معلوماتية بمجرد فقط استخدام الحاسوب أداة للعمل بها (3). وقد اتخذ نظام مكافحة الجرائم المعلوماتية السعودي لسنة 2007 هذا الرأي لتعريف تلك الجرائم حيث عرفها بأنها " أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام " (4).

الرأي الثاني : تعريف الجرائم المعلوماتية بالاستناد إلى موضوعها عرف البعض هذا النوع من الجرائم المعلوماتية بأنها " مجرد نشاط موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه (5). كما عرفت هذه الجرائم أيضاً بأنها مجموعة الجرائم المتصلة بعلم المعالجة المنطقية للمعلومات (6). وتعرف

1- د.عبدالفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي ، ط1، دار الكتب القانونية ، المحلة الكبرى ، 2007 ، ص 24.

2- د.هلالي عبد اللاه أحمد ، التزام الشاهد في الجرائم المعلوماتية ،ط1، دار النهضة العربية ، القاهرة 1997، ص3.

3- د. أيمن عبد الله فخري ، جرائم نظم المعلومات ، دار الجامعة الجديدة ، الاسكندرية ، 2007، ص 85.

4- د. عبد الفتاح بيومي ، مرجع سابق ، ص 24.

5- سامي علي حامد عياد ، الجريمة المعلوماتية واجرام الانترنت ، دار الفكر الجامعي ، 2007 ، ص 27.

6- د. مكي احمد عبد الزعبي ، حق الخصوصية في القانون الجنائي ،ط1، المؤسسة الحديثة ، لبنان ، 2006، ص 3.

كذلك كل سلـــوك غير مشروع معاقب عليه قانوناً صادر عن إرادة جريمة محله معطيات الحاسب [1]. وقد عرفها مجموعة من الخبراء خلال مؤتمر عقد في باريس سنة 1983 حول الجرائم المرتبطة بالمعلوماتية بأنها سلوك غير مشروع أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها [2] ، وقد اعتبره البعض بأنه أفضل تعريف وشامل وواسع ويمد نطاق التجريم إلى الأخلاق التي تخرج عن نطاق التجريم في القانون [3].

الرأي الثالث: تعريف الجرائم المعلوماتية بالاستناد إلى المعرفة الفنية باستخدام الحاسوب في التعريف بالجرائم المعلوماتية ، وقد ورد في هذا الرأي عدة تعاريف منهما من يرى أن الجرائم المعلوماتية تحتاج لخبرة في مجال الحاسوب [4] كذلك عرفت بأنها أي فعل مشروع تكون المعرفة بتقنية الحاسوب أساسية به وللتحقيق فيه وملاحقته قضائياً.

الرأي الرابع: التعريف المستند على أداة ارتكاب الجريمة وموضوعها معاً. يرى مشجعو هذا الرأي الاعتماد على معيار مزدوج إذ عرفوا الجرائم المعلوماتية بأنها أي عمل لا يوجد له في القانون أو العرف جزاء ويضر بالأشخاص والأموال ويوجه ضد التقنية المتقدمة لنظم المعلومات [5] ، وكذلك يتم تعريفها بأنها كل فعل أو امتناع عمدي ينشأ عن استخدام غير مشروع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال المادية أو المعنوية [6] وقد تكون هي عمل أو امتناع يأتيه يضر بمحتويات الحاسب الإلكتروني سواء

1- د. نائل عبد الرحمن صالح ، واقع جرائم الحاسوب في القانون الأردني ، بحث مقدم الى المؤتمر دبي الإمارات ، ص 3.

2- د. محمد عبدالله أبوبكر ، موسوعة جرائم المعلوماتية ، المكتب العربي الحديث ، الاسكندرية ، ص 12.

3- د. أيمن عبد الله فكري ، مرجع سابق ، ص 86.

4- أسامة أحمد المناعسة ، جرائم الحاسب الآلي ، دار وائل لنشر والتوزيع ، عمان 2001 ، ص 76.

5- د. محمد عبد الله أبو بكر ، موسوعة الجرائم المعلوماتية ، مرجع سابق ص 11.

6- د. أحمد خليفة الملط ، الجرائم المعلوماتية ، مرجع سابق ، ص 86.

المادية أو المعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها [1].

وبعد الانتهاء من سرد المعلومات والآراء في تعريف النظم المعلوماتية نجد أنه من الصعوبة الأخذ بتعريف واحد للجرائم المعلوماتية وذلك لتداخل المعلومات حسب الرأي الأول بين الجرائم المعلوماتية والتقليدية. أما في الرأي الثاني والذي يصب اعتماده على محل الجريمة كأساس للتعريف بالجرائم المعلوماتية فهو رأي غير كاف ، أما الرأي الثالث الذي يقول إنه المعرفة الفنية باستخدام الحاسوب وبالتالي فإنه يجب البحث في الظروف الشخصية للجاني وهذا ما لا يعتد به القانون. وقد أخذ مؤتمر الأمم المتحدة العاشر لمنع الجريمة الذي عقد في فينا عام 2000 بهذا الاتجاه إذ عرّف الجرائم المعلوماتية " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة المعلومات أو شبكة حاسوبية أو داخل نظام حاسوبي أو شبكة حاسوبية داخل نظام حاسوبي ، والجريمة هنا تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية [2].

المطلب الثاني – خصائص الجرائم المعلوماتية:

هناك خصائص تتميز بها الجرائم المعلوماتية عن الجرائم العادية التقليدية ، هذا ولعل أبرز هذه الخصائص هي ما يلي :

أولاً – الجرائم المعلوماتية العابرة للحدود:

يعتبر القيام بفعل أو الامتناع عنه الذي يقوم به الإنسان عن طريق نظام معلوماتي معين [3] قد يكون اعتداء على حق أو مصلحة أو بيانات معلوماتية يحميها القانون أو إضرار بالمكونات المنطقية للحاسوب أو بنظام الشبكات المتصلة به ماساً بحدود أكثر من

1– د. أحمد سامي الشوا، ثورة المعلومات وانعكاسها على القانون في قانون العقوبات.

2– نهلة عبد القادر المومني ، الجرائم المعلوماتية ، ط1، دار الثقافة ، عمان 2008، ص 50.

3– انظر المادة الأولى من اتفاقية بودابست لمكافحة الجرائم المعلوماتية.

بلد نكون أمام جريمة عابرة للحدود [1] أن ما يميز الجرائم المعلوماتية أنها غير مقيدة بمنطقة جغرافية معينة ، إذ ممكن أن ترتكب جريمة من هذه الجرائم خلال وقت معين وفي أي لحظة نظراً لتباعد المسافات ، ويتم ذلك عن طريق الشبكة المعلوماتية التي يتم وصل الحواسيب بينها وعن طريق الانترنت ، أو يبقى حدود الجريمة المعلوماتية فقط في حدود الدولة ، وهذا لا يؤثر في القانون الوطني لأنه يغطي هذا الموضوع قانونياً ، وبالخصوص في الإجراءات المتعلقة بكشف الجريمة مثل التفتيش والقبض على الجاني. وقد نصت اتفاقية بودابست لمكافحة الجرائم المعلوماتية على التعاون الدولي بين الدول الأعضاء لمكافحة هذه الجرائم العابرة للحدود فيما يتعلق بتسليم المجرمين والمعاونة القضائية وغيرها من الإجراءات [2].

ثانياً – الصعوبة في اكتشاف هذا النوع من الجرائم وإثباتها :

هناك الكثير من الأسباب تصعب الاكتشاف والإثبات في الجرائم المعلوماتية ونوجزها في الآتي :

1. أن هذا النوع من الجرائم المعلوماتية لا تترك آثاراً مادية ملموسة في محيطها ، بل ترتكب في الخفاء دون أي آثار كالجرائم التقليدية.
2. مما لا شك فيه أن المجني عليه في الجرائم المعلوماتية عادة يتجنب الإبلاغ عن هذه الجرائم ، ولعدة أسباب منها عدم قدرته الفنية التي تمكنه من اكتشاف الجريمة أو خوفاً من الإضرار بمصالحه ، لا سيما إذا وقعت الجريمة على مؤسسات مالية ومصرفية أو تجارية كبيرة فربما يؤدي الإبلاغ عن الجريمة إلى تأثر المؤسسة أو مركزها المالي إلى خسائر [3].

1- د. هلالي عبد اللاه ، جرائم المعلوماتية عابرة الحدود ، دار النهضة ، ط1، 2007، ص 31

2- انظر اتفاقية بوابست للجرائم المعلوماتية في 2001/11/23 ، المجر.

3- محمد أحمد عباينة ، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة ، عمان ، 2006 ، ص 37.

3. سهولة إزالة أدلة إدانة الجاني خلال فترة بسيطة وبالتالي اختفاء الأدلة بسهولة [1].
4. قلة الخبرة الفنية وذلك لأن هذا النوع من الجرائم يتطلب خبرة فنية عالية وإلماماً واسعاً باستخدام الحاسوب [2].

ثالثاً – الجرائم المعلوماتية جرائم ناعمة:

تتميز الجرائم المعلوماتية بأنها جرائم ناعمة ، لا يتطلب منها أي نوع من المجهودات العضلية ، مثل الجرائم التقليدية كالسرقة والاغتصاب والقتل ، بل أنها تحتاج إلى القدرة الذهنية والعقلية للجاني ، وإلمامه الجيد بتقنيات الحاسوب بحيث تمكنه هذه الميزات من ارتكاب الجريمة وخلال لحظات دون أن يترك أثراً [3].

وهناك عدة خصائص يتميز بها المجرم المعلوماتي تميزه عن غيره من المجرمين العاديين ، ويمكن حصر هذه الخصائص في الآتي:

1. المجرم المعلوماتي المتخصص: أكثر المجرمين في الجرائم المعلوماتية متخصصون في تكنولوجيا الحاسوب وتمكنهم قدراتهم الفنية في التعامل مع الحاسوب من ارتكاب الجريمة المعلوماتية بسهولة وفي وقتٍ قصير [4].
2. العود في هذه الجرائم : يعود معظم المجرمين في الجرائم المعلوماتية لارتكاب جرائم مرة أخرى في مجال الحاسوب إما لشغفهم بالمعلومات [5] أو حصولهم على الأرباح أو إضراراً بالغير [6].

1- محمد حماد مرهج الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، ط1 ، دار الثقافة ، عمان ، 2004 ، ص 166.

2- محمد حماد مرهج الهيتي ، مرجع سابق ، دار المناهج ، عمان ، 2006 ، ص 215.

3- أسامة احمد المناعسة وآخرون ، مرجع سابق ، ص 107.

4- د. عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 83.

5- الجرائم المعلوماتية مصطلح استخدمه لأول مرة (ميخايلوف) مدير المعهد الإتحادي للمعلومات.

6- د. عبد الفتاح بيومي ، مرجع سابق ، مكافحة جرائم الانترنت ، ص 83.

3. تعدد الذين يشتركون في الجريمة : مما لا شك فيه أن الجرائم المعلوماتية تتطلب اشتراك أكثر من شخص واحد في هذه الجريمة ، فقد يكون أحدهم هو المحرض أو المخطط لارتكاب الجريمة. ويتضح لنا أن الجرائم المعلوماتية لها خصائص تميزها عن الجرائم التقليدية ، فهي جرائم لا تمر على حدود الدولة ولا يمكن اتخاذ الإجراءات المناسبة لمكافحتها ، إلا بوجود اتفاقيات تعاون قضائي ودولي.

المطلب الثاني – محل الجرائم المعلوماتية:

إن موضوع الجرائم المعلوماتية يعتبر المعلومات هي الأساس الرئيسي لهذه الجرائم ، لهذا السبب لا بد من القيام بدراسة المعلومات بشيء من التعمق والإسهاب ، لهذا السبب سوف نركز في هذا الموضوع في نقطتين مهمتين وهما مدلول المعلومات والنقطة الثانية سوف نتناول خصائص المعلومات بشكل عام والشروط الواجب توافرها فيها لتكون محلاً للحماية القانونية.

أولاً – مدلـول المعلـومات:

إن المعلومات الموجودة حالياً تعتبر هذه الكلمات قد استخدمت قديماً من القرن الماضي في مختلف المجالات ، مما جعل لهذا الاستعمال الشائع مفاهيم متنوعة ومتعددة [1].

أما من الناحية الفقهية فهناك الكثير من التعريفات للمعلومات وضعها الفقهاء حيث عرفت بأنها "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلاً للتبادل والاتصال أو التفسير أو التأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الالكترونية وهي تتميز بالمرونة بحيث يمكن تغيرها وتجزئتها [2].

1- محمد عبد الله أبو بكر سلامة ، مرجع سابق ، ص 71.

2- د. نائلـــة عادل فريد قورة ، جرائم الحاسب الآلي ، الاقتصادية ط1 ، منشورات الحلبي الحقوقية ، بيروت ، 2005، ص 96.

إلا أن من عيوب هذا التعريف أنه يخلط بين المعلومات والبيانات ولا يفرق بينهما إذ أنه عرف المعلومات على أنها بيانات ولم يفرق بينهما ، ومن التعريفات أيضاً " البيانات تعتبر مجموعة من الأرقام والكلمات والرموز أو الحقائق والإحصائيات الخام التي لا علاقة بين بعضها البعض ، والتي لم تخضع بعد لعملية تفسير أو تجهيز للاستخدام والخالية من المعنى الظاهر في أغلب الأحيان ، أما المعلومات فهي المعنى الذي يستخلص من البيانات عن طريق العرف أو الاتفاق أو الخبرة أو المعرفة [1].

مما لا شك فيه أن آخر تعريف قد فرق بين البيانات والجرائم المعلوماتية ، فقد وصف هذا التعريف البيانات بأنها المادة الخام ، التي يتم تحويلها مباشرة إلى جهاز الحاسوب والذي بدوره يحولها إلى معلومات ، ولهذا سميت العلاقة بين البيانات والمعلومات بالدورة الاسترجاعية ، إذ يتم تجميع البيانات وإدخالها ثم بناءً على هذه المعلومات نقوم باستخراج المعلومات كمخرجات من الحاسوب ، وهي نتاج معالجة تلك البيانات آلياً.

وقد استقرت منظمة التعاون الاقتصادي والتنمية عام 1992 والخاصة بأنظمة الحاسوب وشبكات المعلومات ، بالتفرقة الواردة في الاتجاه المقابل حيث عرفت التوصية البيانات بأنها مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلاً محدداً يجعلها قابلة للتبادل والتفسير أو المعالجة بواسطة الأفراد أو بوسائل الكترونية. أما المعلومات فهي المعنى المستقى أو المستخلص من هذه البيانات [2].

هناك جانب من الفقه يرى أنه لا يوجد حد فاصل ودقيق بين البيانات المدخلة وبين المعلومات المستخرجة من الحاسوب وذلك لأن التداخل موجود بينهما فما يعد معلومات

1- د. هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، اسيوط 1994 ، ص 25 وما بعدها.

2- محمد عبد الله أبو بكر ، مرجع سابق ، ص 72.

مخرجة من الحاسوب قد يكون في مرحلة لاحقة بيانات إذا أجريت عليها معالجات آلية عن طريق الحاسوب وذلك بإدخالها إلى الحاسوب مرة أخرى [1].

لم تقم اتفاقية بودبست بالتفرقة بين المعلومات والبيانات واستخدمت الاتفاقية الكلمتين كمترادفين للمعنى نفسه اذ عرفت الفقرة ب من المادة الأولى البيانات المعلوماتية بأنه "كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل وتكون مهيئة للمعالجة الآلية بما في ذلك برنامج معد من ذات الطبيعة ، يجعل الحاسب يؤدي المهمة" [2] وتشير المذكرة التفسيرية للاتفاقية إلى أن هذا التعريف مأخوذ من هيئة التوصيف العالمية الآيزو. ويتطلب هذا التعريف أن تكون البيانات والمعلومات في وضع يتمكن مستعمل الحاسوب من معالجتها عن طريق الجهاز ، ويتضح من التعاريف السابقة أنه لا يوجد فرق بين البيانات والمعلومات بحيث أن كل من الجهتين يجب أن يخضع للحماية القانونية فالبيانات عبارة عن معلومات وأرقام يتم تغذية الحاسب بها ومن ثم الحصول على مخرجات من الجهاز.

ثانياً – خصائص المعلومات:

تتميز المعلومات بصورة عامة بعدة خصائص تمكن من التعرف على طبيعتها وقدر أهميتها والحماية اللازمة لها ، وتقسم هذه الخصائص إلى قسمين الأول يمكن تسميته بالخصائص الأولية للمعلومات ، أما الثانية فهي الخصائص التكميلية للمعلومات:

المعلومات باعتبارها نوعاً من المعرفة:

يكتسب الإنسان المعرفة بشكلٍ عام من المعلومات التي يتم اكتسابها عن خبرته الإنسانية والدراسية [3] ومما لا شك فيه أن المعرفة تختلف عن نوع آخر من المعلومات

1- د. علي أحمد عبد الزعبي ، مرجع سابق ، ص 301.

2- ISO هو هيئة التوصيف العالمية وهي دولية تأسست عام 1947 لوضع المواصفات وتمثيل فيها الدول بهيئات التوصيف الاقليمية بهدف توحيد المواصفات على المستوى العالمي ، لمزيد من التفاصيل على المستوى العالمي ،انظر ندوة التطورات الحديثة من نظم ادارة الجودة.

3- محمد عبد الله ابو بكر ، موسوعة جرائم المعلوماتية ، مرجع سابق.

يطلق عليه تعبير Knowledge والذي لا يمكن التوصل إليه ومعرفته عن طريق الخبرة العادية أو الدراسية ، وهذا ينطبق على المعلومات في مجال تكنولوجيا المعلومات والمستخدمة في الحاسبات الآلية ودوائر الاتصالات دون أن يتمكن أي شخص من قراءتها أو معرفتها مثال ذلك النتائج التي تتوسط العمليات الحسابية أي مراحل العملية الحسابية قبل الوصول الى النتيجة النهائية وينطبق هذا الوصف على جميع المعلومات المشفرة [1].

المعلومات التي تتخذ شكل التعليمات في مجال تكنولوجيا الحاسبات الآلية:

يعتبر هذا النوع من المعلومات ذا أهمية في مجال تكنولوجيا الحاسوب ، إذ تكون هذه المعلومات على شكل برامج لتشغيل الحاسب الآلي ، وقيامه بالمعلومات المطلوبة ، هذه المعلومات يمكن أن تكون هدفاً للجريمة الالكترونية [2] ويمكن التلاعب بها ، ويصعب أحياناً كشف هذا التلاعب [3].

المعلومات المتعلقة بقطاع المال والأعمال:

تزايد قطاع المال والأعمال اعتماده على تكنولوجيا الحاسوب لما توفره هذه التكنولوجيا من جهد ووقت ومن أهم هذه الأمثلة على المعلومات المتعلقة بهذا القطاع :

أ- سرية المعلومة بسبب أهميتها الكبرى حتى لا يستفيد منها المنافسون [4].

ب- المعلومات المالية وهي تلك المعلومات المتعلقة بالمركز المالي لقطاعات الأعمال المتنوعة ، وهذه المعلومات يجب أن تكون صحيحة وموثوقة المرجع.

ت- المعلومات المتعلقة بالإنتاج : يحرص أصحابها على الحفاظ على سرية خطوات إنتاجهم.

ث- المعلومات الفكرية: كالكتب وبرامج الحاسوب والأعمال الأدبية والخرائط وغيرها حيث تتكفل قوانين الملكية بحمايتها.

1- د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، مرجع سابق ، ص 101.

2- د. نائلة عادل محمد فريد ، مرجع سابق ، ص 102.

3- محمد عبد الله أبو بكر ، مرجع سابق ، ص 87.

4- البرامج المصدرية وبرامج الهدف نوعان من البرامج تستخدم.

ج- تعدد الإجراءات الأمنية المتخذة لحماية المهمة التي يجب عدم كشفها فالوصول إلى المعلومات المتعلقة بإجراءات الحماية يشكل تهديداً لتلك المعلومات [1].

النقود كنوع من المعلومات في عالم الحاسوب وتكنولوجيا المعلومات:

أصبح استعمال النقود والتجارة الالكترونية في تزايد مستمر وأصبح إبرام الصفقات الكبيرة لتبادل السلع والدفع عبر الانترنت شكلاً مألوفاً.

ثالثاً – الخصائص التكميلية للمعلومات:

من المهم التعرف على الخصائص التكميلية للمعلومات للوقوف على طبيعة خصائص تلك المعلومات ونوع الحماية اللازمة لها ومن أهم خصائصها :

1. مدى إتاحة المعلومة: قد تكون المعلومة متوفرة للجميع أو غير متوفرة إلا بشروط بحيث أنها غير متاحة للجميع.
2. مدى أهمية المعلومة وقيمتها وفائدتها: مما لا شك فيه مطلوب معرفة أهمية المعلومة وقوة قيمتها للتمكن من معرفة مدى الحماية اللازمة لها.
3. معرفة مالك وحائز المعلومة أو من يسيطر عليها.
4. عدد المعلومات ، كعدد الصفحات والكلمات.
5. مصداقية المعلومة ومدى صحتها.
6. مكان وجود المعلومة.
7. أهمية المعلومة من حيث الزمان أي معرفة قيمتها في زمان معين ، وقد تكون هذه القيمة في تناقص في زمان آخر حتى تصبح لا قيمة لها كأسعار الأسهم اليومية والتعاملات اليومية.
8. موضوع المعلومة : أي عنوانها وما يحتوي عليه من تفاصيل.
9. تأثير المعلومة : ويتوقف ذلك على مدى التأثير الذي تحدثه المعلومة أو حيازتها أو استعمالها.

1- د. نائلة عادل محمد فريد قورة ، مرجع سابق ، ص 102.

10. وسائل حماية المعلومة : أي ما هي الوسائل التي تستخدم لحماية المعلومة [1].

المبحث الثاني - ماهية التفتيش في الجرائم المعلوماتية:

يعتبر تمسك الفرد بمستودع سره حق له باعتبار أن أسرار الإنسان تخصه وحده فقط وهذه الأسرار جزء مهم من حياته اليومية ، ومن هذا المنطلق يحق للفرد التمسك بأسراره الشخصية وعدم انتهاكها سواء كان ذلك في مسكنه أو مراسلاته أو معلومة مخزنة في جهاز الحاسب الآلي الخاص به أو نظامه المعلوماتي ، ولهذا فله الحق بالتمتع بحماية القانون لهذا الحق ، الذي يعتبر من الحقوق الدستورية لهذا المواطن التي لا يحق لأحد انتهاكها دون سبب قانوني ، ولكن قد يتطلب في بعض الأحيان انتهاك هذا الحق وكشف السرية من أجل الوصول إلى الحقيقة التي يتطلبها القانون وهذا الخرق يكون بموجب إجراء نص عليه القانون وهو التفتيش. وسوف نقسم هذا المبحث إلى مطلبين الأول يتناول تعريف معنى التفتيش القضائي وخصائصه وتفتيش الدليل الالكتروني أما في الثاني فسوف نتناول فيه بعض صور التفتيش غير القضائي.

المطلب الأول – تعريف التفتيش الالكتروني وخصائصه:

أولاً: التفتيش لغة : فتش الشيء فتشاً وفتشه تفتيشاً [2] ، أما معناه اصطلاحاً (اجراء تقوم به السلطة القضائية للاطلاع على محل يتمتع بحرمة خاصة للبحث عن الأدلة اللازمة للتحقيق الجنائي) [3]. وهناك الكثير من التعريفات الاصطلاحية ذكرها الفقهاء مثل أنه (إجراء من إجراءات التحقيق الابتدائي التي تهدف إلى البحث عن الأدلة المادية الجنائية سواءً لجناية أو جنحة تتحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقط لإجراءات قانونية محددة [4].

1- د. نائلة عادل محمد فريد ، مرجع سابق ، ص 108 وما بعدها.

2- الامام محمد بن أبي بكر الرازي ، مختار الصحاح بدار الكتاب العربي ، بيروت 1981 ، ص 49.

3- د. توفيق الشاوي ، حرمة الحياة الخاصة ونظرية التفتيش ، منشأة الاسكندرية ، 2006 ، ص3.

4- د. هلالي عبد الله احمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، ص 430.

ثانياً: مما لا شك فيه أن محل التفتيش في الجرائم الالكترونية وجرائم المعلومات هو جهاز الكمبيوتر والأجهزة المتصلة به والشبكة العنكبوتية والتي تشمل في مكوناتها مقدم الخدمة والمزود الآلي والمضيف والملحقات التقنية وهذا يعني ان التفتيش سوف ينصب على المكونات الآتية :

1. مكونات مادية Hardware وأخرى منطقة Software أو ما يصطلح على تسميته بالقطع الصلبة والبرمجيات.
2. شبكات اتصال بعدية Networks telecomm-unication سلكية ولا سلكية.

أ- تفتيش المكونات المادية لجهاز الكمبيوتر :

ليس هناك خلاف على أن الولوج إلى المكونات المادية للكمبيوتر بحثاً عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش ، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك ، وهل هو من الأماكن العامة ، أو من الأماكن الخاصة حيث أن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمة ، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانوناً في التشريعات المختلفة (1).

ولنا رأي في موضوع تفتيش جهاز الحاسب الآلي وهو أنه أصبح هناك الكثير من الأجهزة الحديثة غير الكمبيوتر بها معلومات نفس المعلومات الموجودة في الحاسب الآلي ولا تنقل عنه بل المعلومات الحديثة زادت في هذه الأجهزة ، مثل الآيباد ، والآيفون ، وغيره من الأجهزة المحمولة ، فإلى أي نوع من التفتيش تخضع هذه الأجهزة وبالذات اذا كانت محمولة مع المتهم في جيبه مثلاً ، ولهذا نرى أن تفتيش المسكن لا يكفي في جرائم

1- د. هلالي عبد الله احمد ، تفتيش نظم المعلومات وضمانات المتهم المعلوماتي ، مرجع سابق ، ص 73.

المعلوماتية وإنما مطلوب تفتيش الأشخاص أيضاً ، لأنه إذا كانت المعلومات تأتي إلى شبكة الإنترنت فإنها قد تأتي لتلفونات محمولة مثل الآيفون الذي يحمله الشخص في أي مكان.

(ب) تفتيش المكونات المنطقة (البرامج Software) للحاسب الآلي:

ثار خلاف كبير في الفقه بشأن جواز تفتيشها فذهب رأي في الفقه إلى جواز ضبط البيانات الالكترونية بمختلف أشكالها ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط أي شيء فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة [1] وغير المحسوسة.

بينما يرى رأي آخر عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة ، ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الكمبيوتر بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب الآلي [2] وفي مقابل هذين الرأيين يوجد رأي آخر اختلف عنهما حيث نأى بنفسه عن البحث عما إذا كانت كلمة (شيء) تشمل البيانات المعنوية لمكونات الكمبيوتر أم لا ، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي والذي يتطلب أن يقع الضبط على بيانات الحاسب الآلي إذا اتخذت شكلاً مادياً [3].

(ت) تفتيش الشبكات المتصلة بالكمبيوتر (التفتيش عن بعد):

أصبحت أعمال التفتيش والضبط صعبة ، لكون سلبية التكنولوجيا الرقمية قد عقدت من التحدي أمام أعمال التفتيش والضبط فالبيانات التي تحتوي على أدلة قد تتوزع عبر

1- د. هلالي عبد اللاه احمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلـوماتي ، مرجـع سابق ، ص 73.

2- Piragoff (donllatk) computer crimes and other crimes against information technology in canada , op cit P241.

3- د. هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي ، مرجع سابق ، ص 84.

شبكات الحاسوب في أماكن مجهولة بعيدة تماماً عن الموقع المادي للتفتيش وإن ظل من الممكن الوصول اليها من خلال حواسب تقع في الأبنية الجاري تفتيشها.

وقد يكون الموقف الفعلي للبيانات داخل اختصاص آخر في حين أن السلطات في بعض البلاد قد لا تنزعج من أن تقودها تحقيقاتها الكترونياً إلى اختصاص قضائي آخر إلا أن السلطات في ذلك الاختصاص السيادي قد تشعر ببالغ الانزعاج وهذا يزيد التعقيد من مشاكل الجريمة المعلوماتية العابرة للحدود ويزيد من أهمية تبادل التعاون القضائي [1] وهناك ثلاث صور لهذا الموضوع :

الصورة الأولى : اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة مكان آخر داخل الدولة.

الصورة الثانية : اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة.

وتعتبر هذه الصورة من الصور المهمة في التفتيش الالكتروني حيث تواجه مشاكل السلطة التي تقوم بالتفتيش في جمع الأدلة والتحقيقات في حالة امتداد الإذن بالتفتيش في جمع الأدلة والتحقيقات في حالة امتداد الاذن بالتفتيش إلى خارج الدولة أي إقليمها الجغرافي التي صدر من جهتها المختصة الاذن ودخوله في المجال الجغرافي لدوة اخرى وهو ما يسمى بالتفتيش عبر الحدود ، فقد يتعذر القيام به بسبب امكانية تمسك كل دولة بسيادتها وحدودها الاقليمية [2] ، أما الاحتمال الثالث : فهو التنصت والمراقبة الالكترونية لشبكات الحاسب الآلي.

1- د. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، مرجع سابق ، ص 203.

2- Siebet Ulrich, computer crime and other crime against information technology commentary and preparatory question of the A.I.D.pin 1999.

المبحث الثاني - شروط تفتيش النظام المعلوماتي للحاسب الآلي:

بما أن التفتيش يعتبر من إجراءات التحقيق الابتدائي الخطيرة التي تمس الحرية الشخصية وتنتهك مستودع سر الإنسان وراحته وهدوءه كان لا بد أن يتم وضع قيود وضوابط لتنظيم التفتيش لكي يضمن عدم التجاوز على حرية الأشخاص وحرمة منازلهم إلا في إطار حاجة التحقيق. ويوجد نوعان من الشروط التي يستلزم توافرها لضمان صحة التفتيش وهي الشروط الموضوعية والمتعلقة بسبب التفتيش ومحل التفتيش والجهة القائمة به وسوف نتناول هذا الموضوع في مطلب أول وفي المطلب الثاني سوف نتطرق إلى الشروط الشكلية للتفتيش.

المطلب الأول – الشروط الموضوعية لتفتيش النظام المعلوماتي:

يمكن حصر الشروط الموضوعية لتفتيش النظام المعلوماتي للحاسب الآلي في عدة أسباب ويمكن إجمالها فيما يلي :

الشرط الأول – وجود سبب لتفتيش النظام المعلوماتي:

يعتبر الاذن بالتفتيش اجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة، جناية أو جنحة واقعة بالفعل وترجح نسبتها الى متهم معين ، وان هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية وهو ما أقرته محكمة النقض المصرية في حكم لها [1]. وبناءً عليه وتطبيقاً على الجرائم المعلوماتية فانه لا بد ليكون التفتيش مشروعاً أن نكون:

1. بصدد جريمة معلوماتية واقعة بالفعل سواء أكانت جناية أو جنحة.
2. لا بد من اتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة المعلوماتية أو المشاركة في ارتكابها.
3. لا بد من توافر إمارات قوية أو قرائن على وجود أجهزة أدلة معلوماتية تفيد في كشف الحقيقة لدى المتهم [2].

1– طعن – نقض جنائي ، جلسة 1967/10/16 ، مجموعة احكام النقض ، س18، رقم 195، ص 965.

2– د. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، مرجع سابق ، ص 209 وما بعدها.

الشرط الثاني – تحديد محل التفتيش: [1]

المقصود بالشخص كمحل لتفتيش نظم الحاسب الآلي:

الشخص بوصفه محلاً لتفتيش نظم الحاسب الآلي قد يكون من مستغلي أو مستخدمي الكمبيوتر أو من خبراء البرامج ، سواء أكانت برامج نظام أو برامج تطبيقات ، وقد يكون من المحللين أمن مهندسي الصيانة والاتصالات ، أمن مديري النظم المعلوماتية أو من اي اشخاص اخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حاسب آلي محمولة أو تلفونات متصلة بجهاز المودم أو مستندات. وفي جميع الاحوال يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي وما يتصل به.

المقصود بالمنازل وما في حكمها كمحل لتفتيش نظم الحاسب الآلي:

يقصد بالمنازل وما في حكمها لتفتيش نظم الحاسب الآلي كافة محال الإقامة أو المأوى والملحقات المخصصة لمنافعها والتي يستغلها الشخص سواء بصفة دائمة او مؤقتة وسواء كانت مكونات مادية أو منطقية أو شبكات اتصال خاص ، وعملية التفتيش هنا تخضع لذات شروط وقواعد اجراءات تفتيش المنازل.

السلطة المختصة بتفتيش نظم الحاسب الآلي:

الأصل أن يقوم بإجراء تفتيش نظم الحاسب الآلي سلطة التحقيق الأصلية وهي الادعاء العام – النيابة العامة – كونه إجراء من إجراءات التحقيق وفقاً للقواعد الإجرائية المنصوص عليها في هذا الخصوص.

المطلب الثاني – الشروط والضوابط الشكلية لتفتيش نظم الحاسب الآلي: [2]

بالإضافة إلى الضوابط الموضوعية لتفتيش نظم الحاسب الآلي السالفة الذكر توجد ضوابط أخرى ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء وذلك صوناً

1- المرجع السابق ، ص 314-315.

2- المرجع السابق ، ص 220 وما بعدها.

للحريات الفردية من التعسف أو الانحراف في استخدام السلطة ، ومن أهم هذه الضوابط ما يلي :

1. أن يكون الأمر بالتفتيش مسبباً:

يعتبر من الضمانات المقررة في التشريعات الإجرائية الجزائية تسبيب أمر التفتيش ، ويقصد بالتسبيب أن الأمر الصادر لا بد وأن ينبنى على عدة قرائن ودلائل تدل على أن في المكان المراد أو الشخص المراد تفتيشه ما يفيد في كشف الحقيقة.

2. أن يكون الإذن بالتفتيش مكتوباً:

ويجب أن يتضمن أمر الندب من أصدره ووظيفته وتاريخ وساعة صدوره واسم وأسماء المقصودين بالتفتيش وأن يحدد له فترة معقولة ويمكن تجديدها عند انقضائها بغير تنفيذ ويذيل الأمر من أصدره.

3. اشتراط التوقيع ممن أصدر الإذن وإثبات تاريخه:

اشتراط الكتابة في اذن التفتيش يستتبع بحكم اللزوم ووجوب التوقيع عليه ممن أصدره اقراراً بما جعل منه وإلا فانه لا يعتبر موجوداً. ويضحي عاديا ما يفصح عن شخص مصدره ذلك أن إذن التفتيش ورقة رسمية يجب أن تحمل في ذاتها دليل صحتها ومقومات وجودها بأن يكن موقعاً عليها ، ذلك لأن التوقيع هو السند الوحيد الذي يشهد بصدوره ممن صدر عنه.

4. تحديد نوع الجريمة ومحل التفتيش:

يشترط لإصدار الإذن أن يبين مصدره نوع الجريمة المراد ضبط الأشياء المتعلقة بها ، والتي تفيد في كشف الحقيقة.

5. تحديد مدة الإذن بالتفتيش ونطاقه:

يجب أن يكون إذن التفتيش محدد المدة ويكون مأمور الضبط القضائي ملتزماً بالقيام به خلال هذه الفترة ، ويراعي المحقق عند إصداره الإذن إلا تكون مدته طويلة ، والعلة في ذلك عدم بقاء المأذون بتفتيشه مهدداً في حريته وحرمة مسكنه لمدة طويلة.

6. تحرير محضر بتفتيش نظم الحاسب الآلي:

من حيث أن التفتيش في الأصل يعتبر عملاً من أعمال التحقيق فإنه ينبغي والحال كذلك تحرير محضر به يثبت فيه كل ما تم من إجراءات وما أسفر عنه التفتيش من إدانة.

الفصل الثاني
آثـــار التفتيـــش

التفتيش بوصفه إجراء من التحقيق يمس الحرية الشخصية وحرمة الأماكن كما سبق أن أوضحنا ذلك ، وهو بذلك يهدف إلى الحصول على أدلة الجريمة سواء أكانت أدلة معلوماتية في الجرائم المعلوماتية ، وبهذا يترتب على التفتيش أثر مباشر وهو ضبط الأدلة التي يتم البحث عنها إذا نجم عن التفتيش إيجاد هذه الأدلة ، وضبط الأدلة المعلوماتية يختلف عن ضبط الأدلة المادية في أمور كثيرة كما سنتعرف من خلال المبحث الأول الذي سوف يتناول ضبط الأدلة والذي سوف نقسمه إلى مطلبين : في المطلب الأول سوف نتناول قواعد ضبـــط الأدلة أما في المطلب الثاني فسوف نتحدث عن المراقبة الالكترونية لشبكات الحاسوب [1].

1- يرى البعض من الفقه أن البيانات المخزنة آلياً لا تصلح لأن تكون محلاً للضبط بالكيفية المنصوص عليها في القوانين الإجرائية التقليدية بسبب انتفاء الطابع المادي عن هذه البيانات لمزيد من التفاصيل انظر د. هشام محمد فريد رستم ، الجوانب الاجرائية للجرائم المعلوماتية ، مكتب الآلات الحديثة ، اسيوط ، طبعة 1994 ، ص 194، ونحن من جانبنا نرى امكانية استخدام المعلومات الواردة على الشبكات الاجتماعية ، ولا يحول دون ذلك الطبيعة اللامادية فقد تكون هذه البيانات مسجلة على الصفحات الشخصية او ثابتة في صندوق البريد الخاص بالمجني عليه صادرة من ايميل الجاني وعندئذٍ يجوز نسخ هذه البيانات واسترجاعها وعرضها ، فإذا تبين انها تشتمل جريمة جاز استخدام الدليل الناشيء عن ذلك في الادانة ، فالمشكلة لا تكمن في طبيعة البيانات بقدر ما هي تتعلق بضرورة تأهيل القائمين على الضبط واستلزام تقنيات فنية في ضبط هذه الأدلة ، ويتقارب ذلك الرأي د. عبد الفتاح بيومي حجازي.

المبحث الأول - ضبـط الأدلـة:

يقصد بالضبط هو وضع اليد على الأدوات والأسلحة والأوراق الخاصة بالجريمة ، والتي لها دور في كشف الواقع [1] ، أما الضبط في المجال المعلوماتي فهو وضع اليد على الدعائم المادية المخزنة فيها البيانات الالكترونية أو المعلوماتية المتصلة بالجريمة المعلوماتية التي وقعت وتفيد في كشف الحقيقة عنها وعن مرتكبها [2]. ويوجد نقد على هذا التعريف لأن وضع اليد لا يكون فقط على الدعائم المادية المخزنة فيها المعلومات ، لسبب واحد وهو أن المعلومات قد تضبط أحياناً داخل الشبكة أي عندما تكون في طريقها إلى محل إرسالها ويكون ذلك عند مراقبة الاتصالات الالكترونية ، ويمكن أن نقتـــرح تعريفاً للضبط حيث يرى الباحث "أن الضبط هو وضع اليد على المكونات المادية للحاســوب والأدلة المعلوماتيــة المخزنة في الحاسوب محل التفتيش أو في الشبكة أو في الحاسوب الخـــادم والتي تفيد كشـــف الحقيقة في جريمة وقعت وجاري التحقيق فيها". أن النتيجة الاساسية لإجراء التفتيش هو الضبط في محل الجريمة المعلوماتية سواء أكان هذا المحل جهاز الحاسوب أن الشبكة او المراسلات البريدية الالكترونية ، فالضبط هو الأثر المترتب على الجريمة.

سوف نتطرق في هذا المبحث الى مطلبين ، فنبين في المطلب الأول قواعد الضبط ، أما في المطلب الثاني فسوف نتطرق إلى قواعد التعرف بالمضبوطات.

المطلب الأول - قواعد ضبط الأدلة:

سوف نتحدث في هذا المطلب إلى قواعد ضبط الأدلة سواء كانت قواعد قانونية أم قواعد فنية والتي تضمن الحفاظ على الدليل المعلوماتي من التلف أو التغير وذلك من خلال ما يأتي :

1- د. محمد ابو العلا عقيدة ، شرح قانون الاجراءات الجزائية ، ط2، دار النهضة ، القاهرة ، 2001 ، ص 448.

2- نبيلة هبة هروال ، الجوانب ، مرجع سابق ، ص 266.

أولاً – ضبط المكونات المادية للحاسوب:

إن الهدف هو وضع اليد على الأدلة المادية التي تفيد كشف الحقيقة ، لهذا لا يوجد مشكلة في تطبيق القواعد التقليدية المتبقية في ضبط الأدلة المادية. تتكون مكونات الحاسوب المادية من الحاولية التي تحمل دوائر الكترونية وذاكرته (كيز) لوحة مفاتيح الماوس ، الشاشة ، جهاز الطابعة ، جهاز السكانر ، وغيرها من الملحقات وإذا ما رجعنا الى قانون اصول المحاكمات العراقي نرى أنه قد تطرق إلى ضبط الأدلة الناجمة عن تفتيش في عدد من نصوص هذا القانون [1].

وقد عالج هذا النقص عدد من التشريعات ومنها قانون الإجراءات الجنائية القطري بقوله: "لمأموري الضبط القضائي أن يضعوا الأختام على الأماكن التي بها آثار أو أشياء تفيد في كشف الحقيقة وأن لم يقيموا حرساً عليها ويجب عليهم إخطار النيابة العامة بذلك إذا ما رأت ضرورة ذلك أن ترفع الأمر خلال ثلاثة أيام إلى قاضي محكمة الجنح المختصة لإقراره وإلا اعتبر الإجراء كأن لم يكن ولكل ذي شأن أن يتظلم للقاضي من الأمر الذي أصدره بتأييد القرار أو إلغائه [2].

ثانياً – ضبط الأدلة المعلوماتية:

آثار ضبط الأدلة المعلوماتية خلافاً فقهياً كبيراً بين فقهاء القانون الجنائي:

الرأي الأول: يرى أصحاب هذا الرأي ومعظمهم من الفقهاء الألمان أنه لا يمكن تصور ضبط البيانات المعلوماتية ووضع اليد عليها لأنها ليست ذات مظهر مادي محسوس ، لذلك لا يمكن ضبطها بسبب طبيعتها غير المحسوسة ، ويستند أنصار هذا الرأي إلى المادة 94 من قانون الإجراءات الألماني.

1- انظر نص المادة (83، الفقرة 1) من قانون أصول المحاكمات العراقي.

2- د. هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ، اسيوط ، 1994، ص93.

الرأي الثاني: يرى أنصار هذا الرأي أنه لا يوجد ما يمنع من أن يرد الضبط على البيانات المعلوماتية ، فالفقه الجنائي في بعض الدول يعطي الامكانيات لسلطات التحقيق بالقيام بأي شيء يكون لازماً وضرورياً لجمع وحماية الدليل ومنهم القانون اليوناني والكندي [1].

ثالثاً – ضبط مراسلات البريد الالكتروني:

مما لا شك فيه أن هناك تشابهاً بين الرسائل الالكترونية والرسائل التقليدية وبالتالي مدى إمكانية اخضاع مراسلات البريد وجميع المحادثات السلكية واللاسلكية ، ولا تجيز بعض القوانين ضبط المراسلات التي تمت بين محامي الدفاع والمتهم والخبير الاستشاري وذلك للحفاظ على حقوق الدفاع [2].

ويتضح من النصوص السالفة الذكر أن المراسلات التقليدية إما أن تكون بحوزة المتهم أو موجودة لدى مكاتب البريد فيتم ضبطها من قبل القائم بالتفتيش إذا كانت لها علاقة بالجريمة وهذه المراسلات تكون لها طبيعة مادية ملموسة وهي الأوراق ، وكذلك البرقيات المرسلة عبر الوسائل اللاسلكية على شكل ذبذبات غير مرئية إذ تدون على الورق فيكون لها شكل مادي ملموس ومحسوس ، أما مراسلات البريد الالكتروني فتكون مخزنة على الحاسوب على شكل ملف ، فيمكن تفتيشه أو تخزن الرسالة في صندوق البريد التابع للمتهم.

رابعاً – ضبط الأدلة المعلوماتية التي يتم العثور عليها عرضاً:

قد تتأثر عملية التفتيش أحياناً بحيث يمكن تعثرها في العثور على أدلة معلوماتية غير متعلقة بالجريمة التي يقوم بإجراء التفتيش لأجل ضبط الأدلة التي تفيد كشف الجريمة والحقيقة. يمكن للقائم بالتفتيش أن يقوم بضبط الأدلة التي يعثر عليها بصورة عرضية.

1- د. علي محمود علي حمود ، الأدلة الالكترونية في إطار نظرية الاثبات الجنائي ، بحث مقدم الى المؤتمر العلمي الأول حول الجوانب القانونية ، دبي ، الامارات العربية المتحدة ، 2003 ، ص 14.

2- نص المادة 98 من قانون الاجراءات المصري.

المطلب الثاني – المراقبة الالكترونية:

إن المراقبة الالكترونية تعتبر من الإجراءات الماسة بحرية سرية مراسلاته واتصالاته الالكترونية فالمراقبة الالكترونية تشكل انتهاكاً لذا يجب أن ينظم هذا الإجراء في قواعد قانونية.

أولاً – مفهوم المراقبة الالكترونية:

1. تعريف المراقبة:

تستخـــدم كلمة المراقبة في مراقبة الشبكات الخاصة بالانترنت وقد عرفها قانون المراقبة السلكية واللاسلكية الفدرالي الامريكي بأنها "الالتقاط السمعي ، أو أي التقاط السمعي أو أي التقـــاط لمحتـــويات اي اتصال سلكي أو الكتروني أو شفوي باستخدام أي جهاز آخر" [1].

2. المراقبة الالكترونية وطبيعتها القانونية:

هناك اختلاف في رأي الفقهاء في تحديد الطبيعة القانونية لمراقبة المحادثات الهاتفية والاتصالات الالكترونية حيث انقسمت الآراء إلى ثلاث أقسام وهي :

الرأي الاول: اعتبار مراقبة المحادثات الهاتفية والاتصالات الالكترونية نوعاً من أنواع التفتيش ، وذلك لأن المراقبة مثل التفتيش تشكل انتهاكاً على حرمة الحياة الخاصة للإنسان وحريته الشخصية وعلى أثر ذلك تخضع المراقبة لشروط وضمانات التفتيش [2].

الرأي الثاني: مراقبة المحادثات الهاتفية والاتصالات الالكترونية نوع من أنواع الاطلاع على الرسائل ، يعتبر أصحاب هذا الرأي أن مراقبة المحادثات

1- The wire tap statute section 2510

2- د. قدري عبد الفتاح الشهاوي ، مناط مشروعية العمل الشرطي ، دار النهضة العربية ، القاهرة ، 2007، ص 660.

التلفونية والاتصالات الالكترونية نوع من أنواع الاطلاع على الرسائل لأن الرسالة تتضمن بعض أسرار الحياة الخاصة للمرسل والغير [1].

الرأي الثالث: مراقبة المحادثات الهاتفية والاتصالات الالكترونية إجراء من نوع خاص ، يرى أصحاب هذا الرأي أن مراقبة المحادثات الهاتفية والاتصالات الالكترونية إجراء ذو طبيعة خاصة يماثل التفتيش لكنه ليس تفتيشاً وهو يهدف إلى ضبط الأدلة التي تكشف الحقيقة في جناية أو جنحة وقعت وجاري التحقيق فيها.

الخاتمة والتوصيات

مما لا شك فيه أن للطفرة الهائلة في نظام المعلومات الالكترونية دوراً كبيراً في التقدم العلمي ، ومن هذا المنطلق تم اختيار موضوع التفتيش الالكتروني وما ينتج عنه من مشاكل في الإجراءات ، وقد ذللت بعض هذه المشاكل بعد صدور القانون الاماراتي في مجال المعلومات الالكترونية عام 2012م وبعد كتابة هذا البحث توصلت الى عدة توصيات وهي كالآتي :

1. النظر في إصدار قانون اتحادي إجرائي في مجال الإجراءات مثل التفتيش والقبض وبالذات في المجال الالكتروني لوجود صعوبة في بعض الأحوال في تطبيق قانون الإجراءات في موضوع الادلة الالكترونية مثل خصوصية التفتيش في مجال الأجهزة الالكترونية.
2. تدريب أفراد الشرطة على عمليات ضبط وتحريز الأجهزة الالكترونية وعمل دورات تخصصية لهذا الموضوع.
3. مما لا شك فيه أن للإعلام دوراً مهماً في هذا الموضوع ، وهو عن طريق توعية الجمهور بأهمية هذا الموضوع من ناحية خطورة هذه الأجهزة وأهميتها ، وكيف تنقل المعلومات وكيف يتم سرقتها.

1- د. جمال جرجيس مجلع تاو ضروس ، الشرعية الدستورية لأعمال الضبطية القضائية ، النسر الذهبي للطباعة ، القاهرة ، 2006، ص 464.

المراجع

أولاً - الكتب:

1. د. أحمد خليفة الملط ، الجرائم المعلوماتية ، مرجع سابق.
2. د. أحمد سامي الشوا ، ثورة المعلومات وانعاكسها على القانون في قانون العقوبات.
3. أسامة أحمد المناعسة ، جرائم الحاسب الآلي ، دار وائل للنشر والتوزيع ، عمان 2001.
4. د. أيمن عبد الله فخري ، جرائم نظم المعلومات ، دار الجامعة الجديدة ، الاسكندرية ، 2007.
5. الإمام محمد بن أبي بكر الرازي ، مختار الصحاح بدار الكتاب العربي ، بيروت 1981.
6. توفيق الشاوي ، حرمة الحياة الخاصة ونظرية التفتيش ، منشأة الاسكندرية ، 2006.
7. د. جمال جرجيس مجلع تاو ضروس ، الشرعية الدستورية لأعمال الضبطية.
8. د. خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية.
9. قدري عبد الفتاح الشهاوي ، مناط مشروعية العمل الشرطي ، دار النهضة العربية ، القاهرة ، 2007.
10. د. عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والانترنت.
11. محمد ابو العلا عقيدة ، شرح قانون الاجراءات الجزائية ، ط2، دار النهضة ، القاهرة ، 2001.
12. محمد احمد عياينة، جرائم الحاسوب وابعادها الدولية ، دار الثقافة ، عمان ، 2006.
13. محمد عبدالله ابو بكر ، موسوعة جرائم المعلوماتية ، المكتب العربي الحديث ، الاسكندرية.
14. محمد حماد مرهج الهنيتي ،التكنولوجيا الحديثة والقانون الجنائي ، ط1، دار الثقافة ، عمان، 2004.
15. محمد حماد مرهج الهنيتي، التكنولوجيا الحديثة والقانون الجنائي، دار المناهج ، عمان ، 2006.
16. مكي احمد عبد الزعبي ، حق الخصوصية في القانون الجنائي ، ط1، المؤسسة الحديثة ، لبنان ، 2006.
17. نائلة عادلة فريد قورة ، جرائم الحاسب الآلي ، ط1، منشورات الحلبي الحقوقية ، بيروت ، 2005.
18. نبيلة هبة هروال ، الجوانب.
19. نهلة عبد القادر المومني ، الجرائم المعلوماتية ، ط1، دار الثقافة ، عمان ، 2008.
20. هشام محمد يزيد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، اسيوط ، 1994.
21. هلالي عبد اللاه ، جرائم المعلوماتية عابرة الحدود ، دار النهضة ، ط1، 2007.
22. هلالي عبدا لله احمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي.
23. هلالي عبد الله احمد ، تفتيش نظم المعلومات وضمانات المتهم المعلوماتي.

ثانياً - البحوث العلمية:

1- علي محمود علي حمود ، الأدلة الالكترونية في اطار نظرية الإثبات الجنائي.
2- نائل عبد الرحمن صالح ، واقع جرائم الحاسوب في القانون الأردني ، بحث مقدم الى مؤتمر دبي ، الإمارات.